

Big Brother Watch c. Royaume-Uni (No. 2)

Métadonnées

Mots-clés : Agences de renseignement, Protection des sources

Analyse

Résumé et issue

Dans l'affaire Big Brother Watch et Autres c. Royaume-Uni (No. 2), la Grande Chambre de la Cour européenne des droits de l'homme (CEDH) a conclu que l'article 8(4) et le chapitre II de la loi britannique sur la réglementation des pouvoirs d'enquête (« RIPA ») avaient violé les droits à la vie privée et à la liberté d'expression prévus par la Convention européenne des droits de l'homme (Convention). Les requérants ont contesté la compatibilité de trois programmes de surveillance électronique exploités par le service britannique du renseignement électronique (GCHQ) avec la Convention. Ces programmes sont les suivants : (i) Interception en masse dans le cadre du programme TEMPORA, qui stockait et gérait de grands volumes de données obtenues auprès de leurs détenteurs ; ii) le régime de partage de renseignements avec des pays étrangers, en particulier les États-Unis d'Amérique, par l'intermédiaire des programmes PRISM et Upstream; et iii) l'acquisition de données de communication auprès des fournisseurs de services de communications. Les trois plaintes ont été déposées après les révélations d'Edward Snowden concernant des programmes de surveillance gérés à la fois par les services de renseignement des États-Unis d'Amérique et du Royaume-Uni. La Grande Chambre a estimé que les régimes du Royaume-Uni en matière d'interception massive et d'obtention de données auprès des fournisseurs de services de communications avaient violé la Convention, les défaillances suivantes ayant été détectées : i) l'absence d'autorisation et de contrôle indépendants (les « garanties de bout en bout ») ; ii) l'absence de mention des catégories de sélecteurs dans les demandes de mandat ; iii) absence d'autorisation interne préalable pour les sélecteurs liés à un individu identifiable; et iv) l'État n'a pas examiné, entre autres garanties, des mesures moins intrusives avant d'activer et de mettre en œuvre des programmes de surveillance électronique.

Les faits

L'affaire concernait trois requêtes déposées après les révélations de l'ancien consultant national américain en intelligence informatique Edward Snowden concernant les programmes de surveillance électronique gérés par les services de renseignement du Royaume-Uni et des États-Unis d'Amérique. Ces requêtes sont les suivantes: i) la requête n° 58170/13 présentée par Big Brother Watch, English PEN, Open Rights Group et Mme Constanze Kurz ; ii) la requête n° 62322/14 déposée par le Bureau of Investigative Journalism et Alice Ross ; et iii) la requête no 24960/15 présentée par Amnesty International Limited, Bytes For All, le Conseil national pour les libertés civiles (« Liberty »), l'American Civil Liberties Union, l'Irish Council For Civil Liberties Limited, l'Association canadienne des libertés civiles, l'Initiative égyptienne pour les droits de la personne,

l'Union hongroise des libertés civiles, Privacy International, l'American Civil Liberties Union et le Legal Resources Centre (Les dix organisations de défense des droits de l'homme), toutes contre le Royaume-Uni.

Big Brother Watch et autres c. Royaume-Uni (Requête No. 58170/13)

Le 3 juillet 2013, les requérants dans la première des affaires jointes ont soumis une lettre au Gouvernement dans laquelle ils ont exposé leurs griefs et ont demandé des déclarations selon lesquelles l'article 8 de la RIPA, les articles 1 et 3 de la loi de 1994 sur les services de renseignement et l'article 1 de la loi de 1989 sur les services de sécurité avaient violé leurs droits garantis par la Convention. Néanmoins, le 26 juillet 2013, le Gouvernement a indiqué qu'en vertu de l'article 65(2) de la RIPA, les allégations relatives aux droits de l'homme contre les services de renseignement ne relevaient pas de la compétence de la Haute Cour, mais que les requérants pouvaient porter leurs griefs devant l'Investigatory Powers Tribunal (IPT), tribunal spécialisé instauré par la RIPA et ayant compétence exclusive pour connaître des allégations de violation de l'instrument juridique susmentionné. Toutefois, aucune autre mesure n'a été prise par les requérants à la suite de cette réponse datée du 26 juillet 2013.

Enfin, les requérants ont saisi la Cour Européenne des Droits de l'Homme d'une plainte faisant valoir, notamment, que le régime d'interception massive était incompatible avec l'article 8 de la Convention. A cette fin, les requérants ont notamment soutenu que l'interception massive des communications ne relève pas de la marge d'appréciation de l'Etat car elle n'est ni proportionnée ni nécessaire conformément à l'article 8 de la Convention.

Bureau of Investigative Journalism et Alice Ross c. Royaume-Uni (Requête No.62322/14)

Dans la deuxième des affaires jointes, les requérants n'ont épuisé aucun recours interne car ils ne pensaient pas qu'ils étaient efficaces pour protéger leurs droits consacrés par la Convention. Au lieu de cela, ils ont déposé une plainte devant la Cour Européenne des Droits de l'Homme en faisant valoir que le régime d'interception massive était incompatible avec leur droit à la vie privée (article 8 de la Convention). En outre, les requérants ont affirmé que le régime prévu par l'article 8(4) viole la protection accordée par l'article 10 de la Convention aux communications privilégiées.

Les dix organisations de défense des droits de l'homme c. Royaume-Uni (Requête No. 24960/15)

Les requérants dans la troisième des affaires jointes ont chacun déposé une plainte auprès de l'IPT entre juin et décembre 2013, faisant valoir que les services de renseignement du Royaume-Uni avaient violé les articles 8, 10 et 14 de la Convention en (i) accédant à et en obtenant des communications interceptées par le gouvernement américain dans le cadre des programmes PRISM et Upstream ; et (ii) en interceptant, en inspectant et en conservant des communications et des données dans le cadre du programme TEMPORA. À cette fin, l'IPT a rendu trois jugements le 5 décembre 2014, le 6 février 2015 et le 22 juin 2015, concluant ce qui suit :

a) Le grief PRISM

PRISM est un programme géré par le gouvernement des États-Unis pour cibler et accéder aux informations confidentielles et personnelles des fournisseurs de services Internet. Dans son jugement, l'IPT a estimé que

si les normes régissant les programmes de surveillance électronique doivent être précises et clairement énoncées dans les normes nationales pour être conformes à l'article 8 de la Convention, dans le domaine de la sécurité nationale, il y a moins d'exigences pour s'acquitter de cette obligation juridique, à savoir « qu'il existe des règles ou procédures appropriées dont l'existence est connue du public et reconnue, et que leur teneur est suffisamment dévoilée pour que l'on sache en quoi elles consistent » et que « ces règles ou procédures font l'objet d'un contrôle approprié ». En conséquence, l'IPT a rejeté cet argument. [para. 41]

En ce qui concerne l'affaire introduite par Amnesty International, l'IPT a conclu que des communications par courrier électronique personnel avaient fait l'objet d'interception et d'examen licites sur la base de l'article 8(4) de la RIPA mais que les règles internes du GCHQ relatives à la durée maximale de conservation avaient été méconnues ce qui constituait une violation de l'article 8 de la Convention. L'IPT a toutefois estimé que l'on n'avait pas accédé aux données en question après l'expiration de la date limite de conservation. Il a donc ordonné au GCHQ de détruire toutes les communications qui avaient été conservées au-delà de la durée autorisée et de lui remettre dans un délai de quatorze jours un rapport confidentiel confirmant la destruction des données. Aucune indemnité n'a été octroyée en l'espèce.

Enfin, en ce qui concerne le Legal Resources Centre, L'IPT a conclu que des communications provenant d'une adresse de courrier électronique associée au Legal Resources Centre avaient été interceptées et examinées dans le cadre d'un mandat émis en vertu de l'article 8 (4) de la RIPA. L'IPT a également constaté que certaines procédures internes de sélection avaient été violées, ce qui constituait une infraction à l'article 8 de la Convention. Toutefois, les informations obtenues par le Gouvernement n'ayant été utilisées par le CGHQ d'aucune manière, l'IPT a jugé que le requérant en l'espèce n'avait pas prouvé l'existence d'un préjudice matériel. Par conséquent, aucune réparation n'a été accordée au requérant.

b) Le grief tiré de l'article 8(4)

L'IPT a jugé que les garanties et procédures prévues à l'article 8 4) de la RIPA étaient justifiées au regard de la Convention.

L'IPT ayant partiellement rejeté les griefs des requérants, ils ont également déposé une requête auprès de la Cour Européenne des Droits de l'Homme pour contester la compatibilité des trois régimes de surveillance et de renseignement du Royaume-Uni (le régime d'interception en masse, le régime de partage de renseignements en collaboration avec des gouvernements étrangers et le régime d'acquisition de données de communication auprès des fournisseurs de services de communications avec les articles 8 et 10 de la Convention. S'agissant de l'article 8, les requérants soutiennent que l'interception en masse n'est ni nécessaire ni proportionnée au sens de l'article 8 de la Convention et, en tant que telle, ne relève pas de la marge d'appréciation reconnue aux Etats. En ce sens, les requérants soutiennent également que les communications privilégiées des ONG sont protégées par l'article 10 de la Convention.

Aperçu de la décision

La Grande Chambre a commencé par exprimer deux préoccupations avant de se lancer dans l'analyse du bien-fondé de l'affaire : i) elle doit limiter son examen à la loi en vigueur à la date à laquelle la Cour a examiné la recevabilité des griefs ; c'est-à-dire qu'elle doit étudier la loi sans aucun des amendements introduits après novembre 2017 ; et ii) Les requérants et le Gouvernement n'ayant pas contesté la conclusion de la chambre selon laquelle l'IPT offre désormais un recours effectif (cela n'a pas été le cas dans la jurisprudence précédente) ce qui signifie que dans les circonstances de l'espèce, que les requérants ont épuisé les voies de recours internes au sens de l'article 35 (1) de la Convention.

Article 8 de la Convention

Article 8(4) régime d'interception en masse de communications

S'agissant de l'article 8 de la Convention, les requérants dans les trois affaires jointes ont contesté la compatibilité du régime d'interception en masse avec le droit au respect de leur vie privée. Pour déterminer si l'interception en masse de communications est compatible avec l'article 8 de la Convention, la Grande Chambre a identifié « six garanties minimales » qui doivent être respectées pour assurer le respect et la jouissance du droit à la vie privée lors de la mise en œuvre de programmes de surveillance électronique : « i) la nature des infractions susceptibles de donner lieu à un mandat d'interception, ii) la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées, iii) la limite à la durée de l'exécution de la mesure, iv) la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, v) les précautions à prendre pour la communication des données à d'autres parties, vi) et les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites » [para. 274]. Ces garanties « ont été régulièrement appliquées dans la jurisprudence de la Cour relative aux interceptions de communications, notamment dans deux affaires portant spécifiquement sur l'interception en masse de communications » [para. 274]. Ces deux affaires sont [Weber et Saravia c. Allemagne](#) et [Liberty et autres c. Royaume-Uni](#). Toutefois, en l'espèce, la Grande Chambre a adapté ces garanties aux circonstances de l'examen pour déterminer si le régime d'interception en masse relève de la marge d'appréciation des États. Selon l'adaptation des « six garanties Weber » effectuée par la Grande Chambre, les juges doivent déterminer si le cadre juridique interne de la surveillance en masse définit clairement : 1) les motifs pour lesquels l'interception en masse peut être autorisée ; 2) les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ; 3) la procédure à suivre pour l'octroi d'une autorisation ; 4) les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ; 5) les précautions à prendre pour communiquer ces éléments à d'autres parties ; 6) les limites posées à la durée de l'interception, la conservation des éléments interceptés et les circonstances dans lesquelles ces éléments doivent être effacés et détruits ; 7) les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement ; 8) les procédures de contrôle indépendant a posteriori du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement. » [para. 361].

Compte tenu de ce qui précède, la Chambre a noté qu'en principe, la capacité des États à mettre en œuvre un régime d'interception en masse relevait de leur marge d'appréciation en vertu de la Convention et de la jurisprudence en la matière. En ce sens, la Grande Chambre a analysé en quoi le régime d'interception massive interfère avec l'article 8 de la Convention quand le régime franchit les différentes étapes du processus d'interception en masse. Cette analyse a aidé la Grande Chambre à comprendre que l'intensité de l'atteinte à l'article 8 de la Convention est croissante au fur et à mesure que chacune des 4 étapes est franchie. Ces 4

étapes sont les suivantes : a) interception et rétention initiale des communications et des données de communication associées (c'est-à-dire des données de trafic qui se rapportent aux communications interceptées) ; b) application de sélecteurs spécifiques aux communications retenues et aux données de communication associées; c) examen par des analystes des communications sélectionnées et des données de communication associées ; et d) rétention subséquente des données et utilisation du « produit final », notamment partage de ces données avec des tiers.» [para. 325].

Si la Grande Chambre a admis que « l'interception en masse revêt pour les États contractants une importance vitale pour détecter les menaces contre leur sécurité nationale », elle a néanmoins identifié trois sujets de préoccupation en rapport avec la mise en œuvre de l'article 8(4) de la RIPA : premièrement, l'absence d'autorisation et de contrôle indépendants du processus, en particulier « le fait que les sélecteurs liés à un individu n'étaient pas soumis à une autorisation interne » ; deuxièmement, l'absence d'identification des catégories de sélecteurs, utilisés dans les recherches, dans les demandes de mandat et l'absence de toute approbation avant leur utilisation ; et troisièmement, l'absence de garanties adéquates applicables à la recherche et à l'examen des données relatives aux communications [para. 424 et 425]. La Grande Chambre a également reconnu la difficulté d'évaluer les systèmes de collecte en masse pour « la surveillance qui ne vise pas directement les individus est par conséquent susceptible d'avoir une portée très large, tant à l'intérieur qu'à l'extérieur du territoire de l'État qui l'opère. Il est donc essentiel autant que difficile de définir des garanties en la matière » [par. 322].

A cet égard, la Grande Chambre a jugé que les lacunes mentionnées ci-dessus rendaient impossible pour le Royaume-Uni de s'acquitter des obligations qui lui incombent en vertu de l'article 8 de la Convention, en particulier l'introduction des « six garanties minimales » mentionnées ci-dessus. Par conséquent, malgré les explications fournies par le Commissaire à l'interception des communications et les recours juridictionnels prévus par l'IPT à toutes les personnes qui pensent que leurs droits humains en vertu de l'article 8(4) ont été violés, les mesures mises en œuvre par le Royaume-Uni, en l'espèce, ont été jugées insuffisantes pour contrebalancer les lacunes susmentionnées. Par conséquent, le régime d'interception en masse prévu à l'article 8(4) de la RIPA ne permettait pas de circonscrire « l'ingérence » au niveau « nécessaire dans une société démocratique », ce qui entraînait une violation de l'article 8 de la Convention [para. 276].

Régime régissant la réception de renseignements provenant de services de renseignement étrangers

Dans la première des affaires jointes, les requérants ont mis en exergue la réception par les autorités du Royaume-Uni de documents interceptés et confidentiels provenant de services de renseignement étrangers. Parallèlement, les requérants dans la troisième des affaires jointes se sont plus spécifiquement plaints de ce que la réception de éléments confidentiels interceptés par la NSA dans le cadre des programmes PRISM et Upstream compromettrait la responsabilité internationale du Royaume-Uni en vertu de l'article 8 de la Convention. Avant de se lancer dans l'analyse, la Chambre a indiqué que son examen se limiterait aux requêtes portant sur la réception « d'éléments d'interception sollicités » auprès de la NSA, ce qui exclut toute prise en compte d'éléments fournis *motu proprio* (de leur plein gré) par des gouvernements étrangers.

Pour déterminer si le Royaume-Uni a enfreint l'article 8 en partageant et en recevant des renseignements interceptés par des services de renseignement étrangers, la Chambre a appliqué une version modifiée ou adaptée des six garanties minimales mises en œuvre lors de l'examen du régime de l'article 8(4). À cet égard, la Chambre a plutôt recherché si les circonstances dans lesquelles le Royaume-Uni pouvait demander des

éléments interceptés étaient circonscrites de manière suffisamment précise et expressément établies par la loi pour empêcher les autorités de se soustraire à leurs responsabilités internationales et nationales. Elle a ensuite appliqué les quatre dernières exigences au traitement dont ces éléments faisaient l'objet une fois que les services de renseignement britanniques les avaient obtenus.

Compte tenu de ce qui précède, La chambre a jugé que la législation interne, assortie des précisions apportées par la modification du code de conduite en matière d'interception de communications, indiquait avec suffisamment de clarté la procédure à suivre pour demander à des services de renseignement étrangers des informations confidentielles. Elle a observé également que rien n'indiquait qu'il y ait eu des défaillances significatives dans l'application de ce régime. Elle a donc conclu qu'il n'y avait pas eu violation de l'article 8 pour ce qui est du régime de réception de renseignements provenant de services de renseignement étrangers.

Régime d'acquisition de données de communication auprès de fournisseurs de services de communications découlant du Chapitre II

Dans la deuxième des affaires jointes, les requérants ont fait valoir que l'obtention de données de communication auprès des fournisseurs de services de communications était incompatible avec leurs droits aux termes de l'article 8 de la Convention. Pour approfondir cette question, la Chambre a considéré que tout régime permettant aux autorités d'accéder aux données obtenues par les fournisseurs de services de communications devrait se limiter à l'obtention d'une autorisation préalable délivrée par un organe judiciaire indépendant dans les cas de prévention « d'infractions graves ».

Tenant dûment compte de la décision de la Cour de justice de l'Union européenne ayant établi que les dispositions de la RIPA régissant la rétention de données des fournisseurs de services de communications étaient incompatibles avec le droit communautaire, la Grande Chambre a conclu que le régime permettant aux autorités nationales d'avoir accès aux données conservées par les fournisseurs de services de communications impliquait une violation du droit au respect de la vie privée. En l'espèce, la Grande Chambre a estimé que l'accès à des documents confidentiels n'était pas soumis à l'autorisation préalable d'un organe judiciaire et qu'il ne visait pas exclusivement à lutter contre les crimes graves, ce qui entraînait la violation de l'article 8.

Article 10 de la Convention

Article 8(4) : régime d'interception massive de communications

Dans la deuxième et la troisième affaires jointes (requêtes no 62322/14 et 24960/15), les requérants ont fait valoir que l'article 8 (4) violait l'article 10 de la Convention en ce qu'il restreignait la liberté d'expression des journalistes et des ONG. Toutefois, la chambre ayant déclaré irrecevable, pour non-épuisement des voies de recours internes, le grief formulé par les requérantes de la troisième affaire, la violation alléguée de l'article 10 n'a été examinée que dans le cadre de la requête déposée par le Bureau of Investigative Journalism et Alice Ross concernant le droit des journalistes à la liberté d'expression et d'opinion.

La Grande Chambre a estimé que les programmes de surveillance en masse en vertu de l'article 8(4) de la RIPA ne visaient ni à accéder aux sources journalistiques ni à surveiller les enquêtes des journalistes, ce qui signifiait qu'en principe, un tel comportement ne pouvait pas constituer une ingérence dans le droit à la liberté d'expression. Par exemple, les services de renseignement auraient pu accéder intentionnellement à des

éléments journalistiques confidentiels en utilisant des mots-clés renvoyant vers des journalistes ou des organes de presse dans le cadre du régime d'interception en masse. Dans ces cas, l'accès aux renseignements personnels ne devrait être accordé qu'après épuisement des garanties juridiques correspondantes établies par la Cour et justifiées par un intérêt public supérieur. Sinon, sans aucune précaution ou arrangement limitant la capacité de l'État contractant d'accéder aux éléments journalistiques confidentiels, une violation de l'article 10 de la Convention est confirmée.

Selon l'article 8 (4) de la RIPA, des éléments journalistiques confidentiels pourraient également être consultés involontairement par les autorités nationales en raison d'une opération d'interception en masse dans laquelle des informations sont recueillies accidentellement. Dans ce cas, l'accès aux éléments journalistiques ne peut être prédit d'emblée ; la participation d'un tribunal indépendant à un stade précoce n'est donc pas possible. Toutefois, si des informations journalistiques confidentielles sont interceptées, il incombe à l'analyste de demander une autorisation judiciaire avant de stocker ou d'examiner ces informations. Cette approbation ne peut être accordée que si l'intérêt public est menacé.

Par conséquent, puisque le Royaume-Uni pouvait accéder à des éléments journalistiques confidentiels et les examiner en justifiant uniquement d'une « exigence impérieuse d'intérêt public », sans établir au préalable (i) des limites quant au moment où ces communications pouvaient être consultées et examinées par les autorités nationales ou (ii) des mesures adéquates pour assurer la protection des informations journalistiques confidentielles, la Chambre a estimé qu'une violation de l'article 10 de la Convention avait été commise en vertu de l'article 8(4) de la RIPA.

Régime régissant la réception de renseignements provenant de services de renseignement étrangers

A cet égard, la Chambre a rappelé que la troisième requête avait été déclarée irrecevable pour non-épuisement des voies de recours internes correspondants. Par conséquent, la Chambre n'a pas examiné ce grief particulier.

En revanche, les requérants dans la troisième des affaires jointes ont contesté la compatibilité du régime d'échange de renseignements avec l'article 10 de la Convention. Toutefois, bien qu'ayant soulevé cet argument en temps utile devant l'IPT, la chambre a estimé que ce grief n'était pas différent de celui introduit par le requérant au titre de l'article 8 de la Convention, qui a déjà été examiné ci-dessus. La Chambre n'a donc conclu à aucune violation de l'article 10 à cet égard.

Régime d'acquisition de données de communication auprès de fournisseurs de services de communications découlant du Chapitre II

Dans la deuxième des affaires jointes, les requérants ont également déposé un grief concernant la compatibilité du régime d'acquisition de données de communications auprès des fournisseurs de services de communications avec l'article 10 de la convention.

Avant de rendre son arrêt, la Chambre a reconnu que le régime du chapitre II offrait une protection accrue lorsque l'accès à des données visait à identifier les sources d'un journaliste. Toutefois, cette protection ne s'appliquait qu'aux demandes visant à identifier la source d'un journaliste, auquel cas une demande d'approbation devait être présentée devant un tribunal national, justifiée par un impératif prépondérant d'intérêt public et devait respecter les procédures prévues par la loi de 1984 sur la police et les preuves en

matière pénale. Cela signifie donc que toute donnée de communication d'un journaliste, autre que ses sources, n'est pas dûment protégée par la législation interne. De plus, il n'y avait pas de dispositions spéciales restreignant l'accès aux données de communication d'un journaliste au but de lutter contre les « infractions graves ». En conséquence, la Chambre a estimé que le régime du chapitre II était contraire à l'article 10 de la Convention puisqu'il n'accordait de protection juridique suffisante qu'aux données portant sur les sources des journalistes.

Opinion commune partiellement concordante des juges Lemmens, Vehabović et Bošnjak

En l'espèce, les juges Lemmens, Vehabović et Bošnjak ont souscrit aux opinions de la majorité sur la plupart des chefs d'accusation. Cependant, ils ont voté contre la décision de la majorité concluant à l'absence de violation des articles 8 et 10 de la Convention lors de l'évaluation du régime de partage des renseignements. En outre, les juges Lemmens, Vehabović et Bošnjak ont estimé que cette affaire constituait une excellente occasion pour la Cour d'affirmer pleinement l'importance de la vie privée dans les questions portant sur la mise en œuvre de programmes de surveillance de masse.

En ce qui concerne la partie dissidente de leur opinion, les juges Lemmens, Vehabović et Bošnjak ont conclu que les programmes de surveillance de masse interféraient avec le droit des individus à la vie privée, tout en restreignant le respect d'autres prérogatives en matière de droits de l'homme telles que la liberté d'association et la liberté d'expression. Par exemple, les juges Lemmens, Vehabović et Bošnjak ont fait valoir que si les individus savaient que les autorités les surveillaient en permanence, ils réfléchiraient à deux fois avant d'exprimer leurs opinions politiques et deviendraient plus prudents dans l'exercice de leurs droits humains.

Parmi leurs arguments, les juges Lemmens, Vehabović et Bošnjak ont, par exemple, souligné le manque de transparence du gouvernement lorsqu'il s'agissait d'expliquer les critères observés pour décider quelles communications doivent être conservées et celles rejetées. Selon les juges Lemmens, Vehabović et Bošnjak, les grands pouvoirs discrétionnaires du Gouvernement pour concevoir le processus de sélection afin d'examiner les documents interceptés doivent susciter la préoccupation de la communauté internationale. Les juges Lemmens, Vehabović et Bošnjak ont relevé également certaines faiblesses au niveau des « six garanties minimales » fournies par la Grande Chambre pour réduire les risques d'abus de pouvoir des États, telles que : i) la capacité de remédier à tout manquement dans le processus d'évaluation globale ; ii) l'absence d'une protection matérielle claire des individus contre les ingérences disproportionnées ; et iii) le fait qu'une définition de ces garanties doit être inscrite dans le droit interne, mais qu'aucune norme minimale ou limitation n'est prévue à cet égard. De même, les juges Lemmens, Vehabović et Bošnjak ont noté que la définition de la « sécurité nationale » donnée par le Commissaire à l'interception des communications était trop large ; par conséquent, elle n'a pas satisfait au critère de la prévisibilité [para. 14].

Opinion partiellement concordante et partiellement dissidente du juge Pinto de Albuquerque

Le juge Pinto de Albuquerque n'a pas pu souscrire à la conclusion de la majorité selon laquelle il n'y avait pas violation des articles 8 et 10 concernant le régime de partage des renseignements, à savoir l'interception en masse par l'Agence nationale de sécurité (NSA) par le biais des programmes PRISM et Upstream. Le juge Pinto de Albuquerque a fondé son opinion, entre autres choses, sur l'inefficacité des programmes de surveillance massive en matière de prévention d'actes de terrorisme. Il a fait valoir que les programmes de surveillance massives constituent un fardeau inutile pour les individus et des restrictions disproportionnées

aux droits à la vie privée et à la liberté d'expression. Par conséquent, à son avis, les États contractants feraient mieux d'investir leurs ressources dans d'autres moyens pour la protection de la sécurité nationale.

De même, le juge Pinto de Albuquerque a fait valoir que la Cour ne disposait pas de tous les éléments de preuve et informations nécessaires pour traiter l'affaire en question de manière adéquate. Par exemple, le Gouvernement n'a pas expliqué à la Cour la portée et l'étendue des sélecteurs et des mots-clés utilisés dans les recherches d'informations confidentielles. En outre, le juge Pinto de Albuquerque a estimé que la Cour avait manqué une excellente occasion de définir clairement les circonstances dans lesquelles des communications privées peuvent être interceptées. Toutefois, en n'abordant pas cette question, la Cour a permis que cette tâche soit confiée aux Parties contractantes. Par conséquent, à son avis, la Cour ne peut pas s'attendre à ce que le gouvernement inclue des garanties juridiques étendues et une définition claire des motifs pour lesquels l'interception massive peut être autorisée, puisque la Cour ne peut pas le faire elle-même.

Dans son opinion en partie concordante et en partie dissidente, le juge Pinto de Albuquerque a également noté que les tribunaux ordinaires devraient être compétents pour superviser l'interception de communications privées dans toutes les interceptions en masse. Selon lui, « la garantie judiciaire doit s'étendre à l'autorisation de la surveillance des communications et des données de communication associées, notamment des données couvertes par le secret professionnel ou par la confidentialité, à la seule exception des cas d'urgence, lorsque le juge compétent n'est pas immédiatement disponible, auquel cas l'autorisation pourra être délivrée par un procureur sous réserve qu'elle soit ultérieurement entérinée par le juge compétent » [par. 24].

En outre, le juge Pinto a suggéré de mettre en œuvre des directives spécifiques et de protéger les informations confidentielles détenues par certains professionnels tels que les responsables politiques, les médecins, les avocats et les journalistes. Enfin, le juge Pinto a appuyé les opinions dissidentes de ses collègues concernant la décision de la Cour de faciliter le partage d'informations confidentielles avec des gouvernements étrangers, car les affaires dans lesquelles des informations ont été fournies d'office par des gouvernements étrangers n'ont pas été évaluées par la Cour.

Opinion commune partiellement dissidente des juges Lemmens, Vehabović, Ranzoni et Bošnjak.

Les juges Lemmens, Vehabović, Ranzani et Bošnjak n'ont pas non plus pu partager l'opinion de la majorité selon laquelle il n'y a pas eu violation des articles 8 et 10 de la Convention en ce qui concerne le régime d'échange de renseignements mis en œuvre par les autorités de l'État défendeur. De l'avis des juges Lemmens, Vehabović, Ranzani et Bošnjak, les mêmes garanties qui s'appliquent au régime d'interception massive devraient également limiter la mise en œuvre du régime de partage de renseignements. De même, selon eux, il ne devrait pas y avoir de distinction dans le traitement des données interceptées, qu'elles aient été demandées ou simplement acceptées par les autorités nationales.

La notion de « garanties effectives », selon eux, implique non seulement l'établissement de dispositions juridiques internes explicites, mais aussi la désignation d'un organe administratif ou d'un tribunal indépendant capable d'assurer une application adéquate de ces dispositions juridiques conformément aux principes fondamentaux de la loi.

Enfin, les juges Lemmens, Vehabović, Ranzani et Bošnjak ont noté que la majorité était d'accord sur le fait que les demandes d'échange d'informations étaient fondées sur des mandats autorisés par le ministre

compétent, mais ils ont considéré que le ministre n'est pas un « organe indépendant » ; ainsi, les mandats utilisés à ces fins ont été approuvés par une « partie intéressée », ce qui a entraîné une violation des obligations internationales de la Partie contractante.

Sens de la décision

Résultat mitigé

L'arrêt élargit la liberté d'expression en ce sens que certains aspects du régime de surveillance de masse du Royaume-Uni ont été jugés inappropriés au sens de l'article 10 de la Convention, en particulier le régime de l'article 8(4) et le régime du chapitre II, discutés précédemment.

Toutefois, la Chambre aurait pu aller plus loin dans son devoir de protéger et de promouvoir la liberté d'expression. Par exemple, la Chambre a admis que le régime de l'article 8(4) relevait de la marge d'appréciation reconnue aux États puisqu'il ne visait pas intentionnellement les journalistes. En d'autres termes, selon les critères de la Grande Chambre, les mesures de surveillance de masse, en général, sont compatibles avec la Convention dans la mesure où elles sont justifiées par une exigence impérieuse d'intérêt public et sont accompagnées des garanties juridiques, autorisations et dispositions correspondantes limitant la capacité de l'État partie d'accéder à des documents privilégiés.

De même, la Chambre a noté que le régime du chapitre II offrait une protection renforcée lorsque des données étaient recherchées pour identifier la source d'un journaliste. Cependant, cela signifie que toute autre information journalistique, tant qu'elle n'implique pas de sources journalistiques, n'est pas protégée. En l'espèce, aucune disposition spécifique ne limitant la capacité du Royaume-Uni d'accéder à l'information journalistique dans le cadre de la lutte contre les « infractions graves », la Grande Chambre a estimé que le régime du chapitre II n'était pas conforme à l'article 10 de la Convention.

Compte tenu de ce qui précède, la Grande Chambre aurait pu saisir cette occasion pour fournir des directives plus précises et détaillées sur les procédures à suivre par les États parties pour examiner, stocker et accéder aux informations privées. Par ailleurs, cette affaire aurait été l'occasion idéale d'exposer les précautions et les mesures que les États doivent prendre lorsqu'ils communiquent des données à des pays étrangers. Toutefois, par son arrêt, la Chambre a permis aux États parties à la Convention de concevoir librement leur système juridique interne en la matière.

La Chambre a également conclu qu'aucune violation de l'article 10 de la Convention n'avait été commise dans le cadre du régime d'échange de renseignements, laissant la porte ouverte à l'échange d'informations privées et confidentielles entre les États parties à la Convention et d'autres pays non soumis au droit européen. En outre, la Cour n'a pas expliqué pourquoi les données interceptées devraient recevoir un traitement différent lorsqu'elles sont demandées par l'État. En ce sens, les informations demandées ou reçues par l'État avec l'aide d'un gouvernement étranger devraient bénéficier du même niveau de protection.

Enfin, en l'espèce, la Grande Chambre a créé une nouvelle norme à suivre par les États parties pour garantir le respect et la jouissance du droit à la vie privée lors de la mise en œuvre de programmes de surveillance



Global Freedom of Expression

COLUMBIA UNIVERSITY

électronique, notamment l'interception massive des communications. Cette nouvelle norme, conçue sur la base des « six garanties Weber », implique que les juges doivent chercher si le cadre juridique national en matière de surveillance de masse définit clairement « (1) Les motifs pour lesquels l'interception en masse peut être autorisée ; (2) Les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ; (3) La procédure d'octroi d'une autorisation; (4) Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés; (5) les précautions à prendre pour la communication de ces éléments à d'autres parties ; (6) Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits; (7) Les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement; (8) Les procédures de contrôle indépendant a posteriori du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement».